VoIP-Sicherheit
Status Quo und neue Aspekte

Johannes Schmitt, Ralf Ackermann, Manuel Görtz, Ralf Steinmetz

Technische Universität Darmstadt
Multimedia Kommunikation (KOM)

{Johannes.Schmitt, Ralf.Ackermann, Manuel.Goertz,
Ralf.Steinmetz}@KOM.tu-darmstadt.de

Zusammenfassung

Das traditionelle Telefonsystem ist aus dem täglichen Privat- und Geschäftsalltag nicht mehr wegzudenken und bietet den Nutzern seit vielen Jahrzehnten ein hohes Qualitäts- und Sicherheitsniveau. Wenn (wie bereits in signifikantem Umfang geschehen [12]) zunehmend IP-basierte Telefonie-Lösungen als Ergänzung oder Ersatz genutzt werden, ist es zwingend notwendig, auch für diese einen Standard sicherzustellen, der eine adäquate Erreichbarkeit, einen stabilen und fehlerfreien Betrieb sowie die Wahrung der Persönlichkeitsrechte, der Abhörsicherheit und des Datenschutzes gewährleistet. Telefonie-Endgeräte, -Server und -Dienste sind oftmals offen über das Internet erreichbar und dadurch ein leichtes Ziel für Angriffe verschiedenster Art. Im vorliegenden Beitrag werden mögliche Risiken, Angriffsarten und -werkzeuge, sowie deren theoretischer Hintergrund aufgezeigt und erläutert. Ebenso werden heute verfügbare Mechanismen zur Verbesserung der Sicherheit analysiert und bewertet. Bewußt bezieht der Beitrag dabei (teilweise durch die Autoren selbst) bereits in der Vergangenheit erfolgte Analysen und die Vielzahl kritischer aber oft nicht umfassend verfügbarer weiterer Aussagen zur behandelten Thematik ein und vervollständigt diese durch eine fundierte Analyse und Darstellung neuer Aspekte.

1 Einleitung

Der nachfolgende Abschnitt ordnet die behandelten Voice over IP (VoIP) Systeme ein und erläutert typische Schutzziele bei ihrer Nutzung.

1.1 Motivation

Der heutige Arbeits- und Privatalltag ist geprägt von der Nutzung vielfältiger Kommunikationsdienste wie E-Mail, Instant Messaging oder dem Informationstransfer über das WWW. Während diese Kommunikationsdienste IP-Netze wie das Internet für den Datenaustausch verwenden, findet die Telefonie weitestgehend immer noch in einem separaten und dedizierten Netz statt. Für eine grundlegende Veränderung, die bereits in signifikantem Umfang begonnen hat, wird der Dienst „IP-Telefonie" – oft auch als Voice over IP (VoIP) bezeichnet – sorgen.

Bedeutung sicherheitsrelevanter Aspekte

Sicherheit und Schutz der Privatsphäre sind grundsätzliche Voraussetzungen für den Ein-

satz von IP-Telefonie im großen Maßstab. Mangelnde Sicherheit und Nicht-Erreichbarkeit bedeuten Vertrauensverlust, stören die Kundenbeziehung und können schließlich zu Umsatzausfällen und Imageverlusten führen. Dennoch hat eine erste Untersuchung von IP-Telefonie-Systemen [4] gezeigt, dass diese sehr anfällig gegen bekannte Attacken (wie beispielsweise das Abhören, Umleiten und Fälschen von Anrufen) sind. Sicherheit wird in vielen Entwicklungen nachträglich in das System integriert, wodurch sich oftmals Bruchstellen ergeben, die für Angriffe genutzt werden können. Neben bekannten allgemeinen Angriffen auf vernetzte IT-Systeme gibt es eine Reihe von spezifischen Attacken auf IP-Telefonie-Systeme. Um die Sicherheit von Voice over IP besser einschätzen zu können, werden daher diese Komponenten und ihre Schutzmechanismen anhand von Gesichtspunkten der IT-Sicherheit im nachfolgenden Beitrag klassifiziert und bewertet.

1.2 Schutzziele in einer Voice over IP Umgebung

Für den vorliegenden Beitrag wurde eine Vielzahl von möglichen Risiken und Angriffsarten betrachtet und bewertet. In einem ersten Schritt werden hier die identifizierten VoIP-spezifischen Angriffe den klassischen Schutzzielen einer IT-Infrastruktur zugeordnet. Für jedes dieser Ziele werden anschließend typische Risiken und Angriffe benannt:

Authentizität: Sicherstellung der vorgegebenen Identität gegenüber einer anderen Entität. Dies ist auf der einen Seite für einen VoIP-Dienstleister als Mechanismus zur Zugriffskontrolle wichtig und stellt sicher, dass vom Nutzer nur Dienste genutzt werden können, für die er auch eine Berechtigung besitzt. Auf der anderen Seite ist die Authentizität des Anrufers ebenso wichtig gegenüber dem angerufenen Teilnehmer. Mögliche Angriffe sind:

- **Phreaking:** Erschleichen kostenloser Telefonate.
- **Identity Theft und Registry Hijacking:** Anmelden an einer Infrastruktur-Komponente unter Nutzung einer fremden Identität.
- **Toll Fraud:** Telefonieren auf fremde Kosten.
- **Session Hijacking:** Übernehmen/Umleiten eines Gesprächs.

Vertraulichkeit: Schutz von Informationen vor dem Zugriff durch nicht berechtigte Entitäten. Signalisierungs- und Mediendaten werden bei der IP-Telefonie teilweise über offene Netze übertragen. Das Mitlesen dieser sensiblen Daten soll verhindert werden. Potenzielle Angriffsarten sind:

- **Call Interception:** Abhören von Telefonaten.
- **VoiceMail Hacking:** Abhören von fremden Voicemails.
- **Violation of Data Privacy:** Sammeln von Benutzerdaten und Informationen über ihr Verhalten.

Integrität und Verbindlichkeit: Gewährleistung, dass die Daten während einer Verbindung nicht abgeändert werden können. Insbesondere die Signalisierung soll vor Manipulation geschützt werden. Dabei ist zu beachten, dass manche Informationen aus den Signalisierungs-Nachrichten nur schwer zu schützen sind, da einige Felder von vermittelnden Entitäten gelesen und teilweise auch modifiziert werden müssen. Damit von einem Dienstleister eine zweifelsfreie Abrechnung genutzter Dienste durchgeführt werden kann, ist es notwendig, dass ein zweifelsfreier Zusammenhang zwischen Nutzer und dessen gesendeten Nachrichten nachvollzogen werden kann. Attacken sind:

- **Dialer:** Manipulation eines VoIP-Telefons um andere Vorwahlen vor der gewünschten Rufnummer anrufen zu lassen.
- **Call Information Manipulation:** Verändern der übertragenen Signalisierungsdaten.

Verfügbarkeit: Garantie, dass benötigte Funktionen und Resourcen zur Nutzung bereitstehen. Ein extrem wichtiges Kriterium bei der Telefonie ist die durchgängige Erreichbarkeit auf der Basis einer zuverlässigen Funktion des Systems. Das Thema Verfügbarkeit erhält zusätzlich Bedeutung, sobald das Voice over IP System auch zum Absetzen von Notrufen genutzt werden muss. Angriffe gegen dieVerfügbarkeit sind:

- **Denial of Service (DoS):** Überlastung von Anmelde- oder Registrierungsdiensten durch (absichtlich) übermässige Beanspruchung.
- **Call Interruption:** Abbruch der Verbindung durch Angreifer.
- **Call Setup Generation:** Aufbau von störenden Anrufversuchen.
- **De-Registration:** Ausnutzen von Schwachstellen im benutzten VoIP-Protokoll, um andere Nutzer abzumelden.
- **SPIT (Spam over IP Telephony):** Versenden von massenhaft Sprachnachrichten – wie etwa zu Werbezwecken.

Strukturelle Schwachstellen: Zusätzlich zu den klassischen bereits genannten Kriterien kommen noch grundsätzliche Schwachstellen in einem System hinzu. Wenn ein Angriff auf diese Schwachstellen erfolgreich war, ist prinzipiell jedes der o.g. Kriterien potenziell betroffen.

- **Endsystem:** VoIP-Endgeräte besitzen oft Funktionalitäten, die über die reine Telefonie hinausgehen. Die Geräte besitzen in der Regel einen über Netzwerk erreichbaren Satz von Funktionen (Netzwerk-Stack, Management-Schnittstellen z.B. über HTTP) was diese anfällig macht für bekannte Schwachstellen in Netzwerkdiensten.
- **Softphones:** Software, welche zum Telefonieren genutzt wird und auf einem allgemein verwendeten Rechner ausgeführt wird, ist potenziell verwundbar durch Trojaner, Würmer und Viren auf dem „Trägersystem".
- **Server-components:** Zentrale Komponenten, wie z.B. Gateways oder Registrars sind in der Regel auf Standard-Hardware und Software aufgebaut. Erkennen Angreifer Schwachstellen auf solchen Systemen, können diese ausgenutzt werden.

1.3 Fazit

Es hat sich gezeigt, dass eine Reihe bekannter Angriffsmöglichkeiten auch für IP-Telefonie-Systeme gelten. Darüber hinaus existieren weitere Möglichkeiten, das System anzugreifen, die spezifisch für diesen Dienst sind. Bei der Sicherung der Systeme gilt es oftmals abzuwägen zwischen der uneingeschränkten Funktionalität und der Abschottung vor fremden Zugriff. So müssen Signalisierungsdaten für ein korrektes Routing lesbar sein, ohne die Signalisierung allen Systemen offenzulegen.

2 Status Quo und neue Herausforderungen

Da sich die Technologien im Bereich VoIP aktuell sehr schnell entwickeln, erscheinen wiederholt neue Protokolle, Protokoll-Varianten, Applikationen und Dienstleister auf dem Markt.

Dadurch stellen sich neue Herausforderungen, diese auf mögliche Risiken und Angriffe hin zu untersuchen und zu schützen.

2.1 Bisherige Situation

Bisher konnten sich zwei Standards im Bereich VoIP durchsetzen. Als erstes fand H.323 als binär-kodiertes, an konventionellen Telefonsystemen orientiertes Protokoll [3] bevorzugt Anwendung – oft als Basis für Telefonsysteme innerhalb von Unternehmensnetzen.

Das Session Initiation Protokoll (SIP) [22] wurde später als textbasiertes, am Format eines E-Mail Headers angelehntes Protokoll entwickelt. SIP dient zum Austausch von Sitzungsinformationen und kann multifunktional eingesetzt werden. Es wird jedoch bisher fast ausschließlich im Bereich VoIP oder im direkten Zusammenhang damit (z.B. Instant Messaging im VoIP-Client) verwendet. SIP findet verstärkt Anwendung im Heimanwenderbereich wie bei VoIP-fähigen DSL Routern, welche eine Nutzung von VoIP mit herkömmlichen Telefonen ermöglichen. Die Übertragung der Mediendaten erfolgt bei beiden Standards über das Real-Time Transport Protocol (RTP, [24]), welches optional durch Nutzung des Real-Time Transport Control Protocol (RTCP) ergänzt werden kann. RTP verwendet zur Übertragung das verbindungslose UDP Protokoll. In der Dokumentation für H.323 und SIP finden sich Vorgaben für Mechanismen zur Sicherung der Kommunikationswege. Deren Schutzwirkungen und Anwendbarkeit in heutigen Systemen werden im Abschnitt 3.3 analysiert.

2.2 Neue Aspekte in VoIP

Bisher fand ein Umstieg auf IP-Telefonie meist innerhalb dedizierter und abgegrenzter Bereiche wie Unternehmen statt. Heute geht der Trend hin zur generellen Nutzung von VoIP als Alternative zur traditionellen Telefonie. VoIP wird nach Studien von Deloitte [12] und BSI [11] bereits heute von ca. 500.000 Nutzern in Deutschland benutzt. Für das Jahr 2007 prognostiziert IDC bereits 15 Millionen Anschlüsse [14]. Die Erwartungen der Nutzer an diese (teilweise nicht einmal bewußt als neuartig wahrgenommene) Technik sind implizit sehr hoch. So werden die gleichen Qualitätsmerkmale wie bei der klassischen Telefonie vorausgesetzt. Um diese Erwartungen zu erfüllen und um im nächsten Schritt VoIP als Ersatz für tradionelle Telefoniesystem zu forcieren, spielen sowohl Verfügbarkeit als auch Sicherheit eine entscheidende Rolle. Diese Sicherheit gilt es auf potenziell unzureichend gesicherten Verbindungen, Endgeräten und vermittelnden Systemen herzustellen. Aktuelle Risiken und Mechanismen, um sich gegen diese abzusichern, werden in diesem Beitrag behandelt – zusätzlich werden folgende neu hinzugekommene Thematiken aufgegriffen:

Spam over IP Telephony - SPIT

Die Sicherung von Verfügbarkeit in einem öffentlichen VoIP-Netz ist neuartigen Herausforderungen gegenüber gestellt. Da Gespräche innerhalb von VoIP bisher meist kostenfrei möglich sind, tritt eine Problematik ähnlich der bei E-Mails auf: unerwünschte Anrufe und Werbebotschaften können durch massenhaftes Auftreten deutlich zu Lasten der Verfügbarkeit gehen und zu einer massiven Belästigung werden. Einige Lösungsansätze werden hierzu in 3.5 vorgestellt.

Neue VoIP Systeme

Neu im Bereich der VoIP Applikationen und Systeme haben sich Asterisk als IP PBX Software mit der eigenen Protokoll-Variante IAX, sowie Skype als VoIP Applikation mit Ansätzen

aus der Peer-to-Peer Technologie etabliert. In den folgenden Abschnitten werden diese Systeme und deren Sicherheitsaspekte vorgestellt.

2.2.1 Asterisk

Im Bereich der VoIP Systeme hat sich mit der IP PBX Software Asterisk ein System weit verbreitet, das sich durch sehr großen Funktionsumfang und die Möglichkeit der Interoperabilität zwischen unterschiedlichen VoIP Protokollen sowie hin zum traditionellen Telefonie-System auszeichnet. Aufgrund dieser Charakteristika wird Asterisk häufig eingesetzt. Das Asterisk-spezifische Protokoll zur Signalisierung und Medienübertragung IAX (InterAsterisk eXchance Protocol) ist dabei jedoch bisher weitestgehend ohne spezielle Sicherheitsvorkehrungen in Verwendung.

Ursprünglich wurde das InterAsterisk eXchance Protocol (IAX/IAX2) zusammen mit dem Telefonserver Asterisk entwickelt. Derzeit ist IAX kein offizieller Standard, sondern vielmehr ein Ergebnis aus der Zusammenarbeit von Open Source-Entwicklern. Der IETF liegt es bisher nur als Draft zur Standardisierung vor. Das IAX-Protokoll ist wie H.323 ein Binärprotokoll. Da IAX für Signalling und Medienströme nur einen einzigen UDP-Port benötigt (5036 für IAX und 4569 für IAX2) lässt es sich, im Gegensatz zu SIP und H.323 basierten Systemen (bei denen es teilweise auch in Abhängigkeit von den verwendeten Infrastrukturelementen und deren NAT-Behandlung zu Problemen kommt), sehr gut in Umgebungen mit Network Address Translation (NAT) einsetzen.

Welche Sicherheitsmerkmale in Asterisk verfügbar sind und welche integriert werden können, wird in 3.4 beschrieben.

2.2.2 Skype

Prinzipiell ist Skype nicht als Protokoll zu bezeichnen, sondern vielmehr als komplette VoIP-Plattform. Das Protokoll, welches die einzelnen Skype-Klienten nutzen, ist nicht offen gelegt. Im Jahre 2003 ist Skype von KaZaa entwickelt worden und beruht hinsichtlich der Signalisierung strukturell auf einem Peer-To-Peer Netzwerk.

Skype hat sich ebenso seinen Platz im VoIP Markt gesichert, jedoch ohne Preisgabe von Implementierungsdetails, so dass es von Interesse ist herauszufinden, ob die Kommunikation über Skype wirklich sicher ist. Einen wichtigen Ausgangspunkt bietet dazu die fundierte Analyse in einem Paper von H. Schulzrinne [5].

Es wird angegeben, dass Skype eine End-to-End Verschlüsselung biete. Wenn man dem Anbieter Glauben schenkt, nutzt Skype eine verschlüsselte Datenübertragung mittels 256-bit AES -auch bekannt als Rijndel. Für die Übermittlung der Schlüssel wird 1536-2048-bit RSA verwendet, wobei die einzelnen Schlüssel der Skype-Nutzer bereits über den zentralen Login-Server authentifiziert wurden.

3 Methoden zur Verbesserung der Sicherheit

Die Umsetzung von Sicherheitsmaßnahmen muss in der Regel auf verschiedenen Ebenen stattfinden, um einen umfassenden Schutz zu gewährleisten (siehe auch [27, 18]). Es muss unterschieden werden zwischen Maßnahmen, welche durch den Dienstleister durchgeführt werden müssen, Maßnahmen, welche den Nutzern angeboten werden müssen, und den Maßnahmen, für die die Teilnehmer selbst verantwortlich sind. Im folgenden Teil werden Schutzmaßnahmen

aufgeführt, welche im Bereich der Netzwerkarchitektur und der Protokolle Verwendung finden. Ein zusammenfassender Überblick über die Mechanismen und ihre Schutzwirkung ist in Tabelle 1 als Zusammenfassung der Ausführungen gegeben.

3.1 Schutz der Netzwerkarchitektur

Schutzmaßnahmen, welche die Netzwerkarchitektur betreffen, werden fast ausschließlich auf der Seite des VoIP-Dienstleisters getroffen. Die Netzwerkinfrastruktur muss grundsätzlich umfassend abgesichert werden. Für die technische Umsetzung von Sicherheitsmaßnahmen innerhalb eines lokalen Netzwerks stehen eine Reihe von Sicherheitsmechanismen zur Verfügung, wie beispielsweise:

- **Anti-Spoofing:** Sicherung von Rechnern gegenüber der Fälschung von DNS Einträgen durch zusätzliche Verifizierung der angegebenen Adressdaten.
- **L2/L1-Sicherheit:** Während Angriffe auf kabelgebundene Netze einen direkte Zugang zum Netzwerk erfordern, ist es möglich, die Kommunikation aller Funknetzwerke (W-LANs) in Reichweite zu belauschen. Insbesondere da diese für mobile Endgeräte zunehmend genutzt werden, müssen W-LAN Schwachstellen abgesichert werden – z.B. durch Nutzung von WPA statt WEP.
- **DoS Protection:** Schutz durch Rate-Limiting, Mehrfach-Handshakes, Redundante Systeme oder Challenge-Response.
- **Stateful-Firewalling:** Abwehren von unerwünschten Zugriffsmöglichkeiten von ausserhalb eines Netzes durch Einsatz geeigneter Firewall Technologien – das dynamische Öffnen von Ports einiger VoIP-Protokolle muss dabei geeignet unterstützt werden.
- **Intrusion Detection/Protection:** Erkennung ungewöhnlicher Vorgänge durch Datenverkehrsanalyse.
- **Authentisierung, Authorisierung und Accounting:** Einsatz von Mechanismen zur Öffnung von Zugängen nur auf Basis sicherer Authentifizierung.
- **Netzwerkstruktur:** Durch logische Unterteilung eines Netzes (VLANs) kann der Telefoniedatenverkehr von „normalem" Datenverkehr (wie E-Mail-, Browser- oder Dateizugriffe) getrennt werden. Dies wiederum erlaubt eine bessere Überwachung.
- **Session Border Controller:** Netzelement zur Verbindung zwischen verschiedenen Netzen. Dient zur Kontrolle im Bereich Sicherheit, Verfügbarkeit und Quality of Service.

3.2 Sicherungsmechanismen auf Protokollebene

Eine weitere Möglichkeit der Sicherung betrifft den Schutz der eingesetzten Protokolle. Dabei lässt sich zwischen einer Ende-zu-Ende-Sicherheit und einer Hop-zu-Hop-Sicherheit unterscheiden. Eine Hop-zu-Hop Sicherung bietet jeweils nur Sicherheit auf dem Weg zwischen zwei Knotenpunkten auf dem Kommunikationsweg und muss sowohl vom Dienstleister als auch vom Nutzer unterstützt werden, um einen umfassenden Schutz zu gewährleisten. Eine Ende-zu-Ende Sicherheit schützt den kompletten Pfad zwischen den beiden kommunizierenden Endsystemen und kann in der Regel ohne Zutun des Dienstleisters durchgeführt werden. Eine Ende-zu-Ende Sicherheit ist jedoch häufig nur begrenzt nutzbar. Zum einen müssen Teile der Signalisierungsnachrichten für den Dienstleister einsehbar sein, um die Nachricht zu verarbeiten und weiterzuleiten. Zum anderen ist der Einsatz von Gateways in andere Netze wie dem

herkömmlichen Telefonnetz in Kombination mit einer Ende-zu-Ende Verschlüsselung bisher nicht möglich. Bekannte Verfahren der Protokollsicherung sind:

- **IPsec:** IPsec [17] authentifiziert oder verschlüsselt die Daten auf der Netzwerkschicht.
- **Virtual Private Network (VPN)-Tunnel:** VPNs sind Tunnel zwischen zwei Knotenpunkten, in denen der Datenaustausch gesichert ist. VPNs bieten sich an, wenn zwei Netze miteinander über eine unsichere Strecke (z.B. das Internet) verbunden werden sollen.
- **TLS:** Transport Layer Security [8] kann als Sicherungsprotokoll auf der Transportschicht eingesetzt werden und stellt die Vertraulichkeit und Prüfung der Integrität zur Verfügung. Darüber hinaus ist mittels des TLS-Handshake-Protokolls eine wechselseitige Authentifizierung möglich.
- **SCTP** Neuere Implementationen von SIP sind in der Lage, das Stream Transmission Protokoll (SCTP) [25] zu verwenden. Dieses verlässliche, verbindungsorientierte Transportschicht-Protokoll ist dazu entworfen worden, Signalisierungsdaten zu übertragen und bietet einen verstärkten Schutz gegenüber DoS Attacken, indem es einen Vier-Wege-Handshake einsetzt.
- **Secure MIME:** S/MIME [20] arbeitet auf der Anwendungsschicht und wird in der Regel für eine Ende-zu-Ende-Sicherheit eingesetzt. Es kann sowohl zur Sicherung der Integrität der Signalisierungsdaten als auch zur Verschlüsselung von Nachrichteninhalten genutzt werden.
- **SRTP:** Der Einsatz des auf digitalen Zertifikaten oder symmetrischen Schlüsseln basierenden Secure RTP [6],[7] schützt den Medienstrom zwischen zwei Geräten.
- **Digest-Authentifizierung/Signatur:** Dieser auch in HTTP genutzte Mechanismus verwendet einen Challenge-Response-Algorithmus (siehe auch [10]) zur Authentifizierung – wird unter anderem in SIP angewendet.

Beispiele für die Nutzung dieser Mechanismen in Form von aufgezeichneten und kommentierten Nachrichten finden sich unter [16].

3.3 Integration in etablierten Systemen

Bei H.323 wird H.235 als bewährter Standard für Sicherheitsmechanismen bei Signalisierungs- und Mediendaten angewendet. Bei H.235 stehen die Authentizität und Integrität der Signalisierungsnachrichten im Vordergrund. Zusätzlich ist in H.235 ein RTP Verschlüsselungsmechanismus definiert.

Das SIP Protokoll sieht für die Authentifizierung eines Nutzers das SIP Digest Verfahren [22] vor, welches nach dem gleichen Prinzip wie das HTTP Digest-Verfahren [10] arbeitet. Nach erfolgter Authentifizierung werden Teile einer SIP Nachricht, welche auf dem Transportweg unverändert bleiben sollen, durch eine Signierung vor Manipulation geschützt. Äquivalent zur Erweiterung des HTTP Protokolls zur Verschlüsselung der Daten auf der Transportebene (Transport Layer Security, TLS) mit der Bezeichnung HTTPS, existiert die Erweiterung des SIP Prokolls mit der Bezeichnung SIPS zur Sicherung der Daten auf dem Transportweg durch TLS. Mittels TLS wird jeweils eine Sitzung auf Transportebene gesichert – d.h. TLS bzw. SIPS ist nur in Kobination mit dem Einsatz von TCP nutzbar. Die Kombination von S/MIME mit SIPS/TLS bietet eine optimale Sicherheit, indem auf dem Transportweg alle Nachrichteninhalte geschützt werden. Für vermittelnde Entitäten sind nur relevante Teile der Nachricht sichtbar und zudem

wird die Integrität gewährleistet. Zudem existiert die Möglichkeit, Mediendaten mittels SRTP verschlüsselt zu übertragen. Oft scheitert dies jedoch an der noch fehlenden Integration dieser Funktion in den Endgeräten oder in den vermittelnden Instanzen.

3.4 Sicherheit in Asterisk

In den bisherigen Versionen unterstützte Asterisk in IAX keine der sicherheitsrelevanten, standardisierten Verfahren wie z.B. das Secure Real-time Transport Protocol oder SIPS. Das Public-Key-Verfahren von IAX2 ermöglicht eine Authentifizierung verschiedener Asterisk-Server mittels RSA-basierender Schlüsselpaare.

In der neuesten Version, welche sich bisher nur im CVS befindet, ist erstmals eine Verschlüsselung integriert. Diese neue Methode bietet die Möglichkeit, eine Verschlüsselung der Daten mittels AES 128bit durchzuführen. Zuvor werden nach einer Challenge-Response Authentifizierung und auf der Basis von Preshared-Keys die Session-Keys generiert, welche zur Verschlüsselung genutzt werden. Verschlüsselt werden dabei die gesamten Frames, wobei die ersten 4 Bytes unverschlüsselt bleiben. In diesen Bytes sind nur solche Daten enthalten, welche benötigt werden, um die Pakete zu transportieren - also die Sender- und Empfängerdaten sowie die Angabe des Frametypes und das Retransmissionsflag.

Bei der aktuell vorliegenden Implementierung ist es also möglich, sowohl Authentizität als auch Vertraulichkeit zu gewährleisten - es gibt jedoch noch Schwachstellen: Die ersten beiden Signalisierungsnachrichten eines Anrufes, welche die Verschlüsselung aktivieren, werden noch unverschlüsselt übertragen und enthalten viele Informationen, die eigentlich nur geschützt übertragen werden sollten: angerufene Nummer, Codec Daten, bevorzugte Sprache oder Benutzernamen.

Versuche, eine SRTP Verbindung in Kombination mit einem Asterisk System als vermittelnde Instanz aufzubauen, scheitern bislang. Asterisk baut initial zu beiden Teilnehmern eines Telefonates unabhängig voneinander eine SIP Verbindung auf und vermittelt sowohl Signalisierungs- als auch Mediendaten zwischen beiden Verbindungen. Das Problem besteht darin, dass die bei Asterisk integrierte Implementierung des SIP-Stacks die für einen Schlüsselaustausch notwendige Informationen (enthalten im Session Description Protokoll/SDP Blocks nicht geeignet an den anderen Teilnehmer weiterreicht und aktuell auch keine implizite Aushandlung der Verschlüsselung im RTP Datenstrom unterstützt wird.

3.5 Mechanismen zur Vermeidung von SPIT

Schätzungen zufolge könnte diese neue Art der telefonischen Kontaktaufnahme bei den Kosten um bis zu drei Größenordnungen billiger sein als traditioneller Telemarketing-„Spam". Der Spitter benötigt vor allem Bandbreite, um Voice Nachrichten zu versenden - eine Nachricht von etwa 15 Sekunden benötigt bei einem Codec mit 64 kbit/s etwa 120 kbyte. Dies ist wenig genug, um Daten im großen Stil zu verschicken, wobei im Gegensatz zum traditionellen Telefonsystem das Versenden von SPIT parallel an eine große Anzahl von Teilnehmern geschehen kann.

Ansätze, wie sie im Bereich E-Mail zu finden sind, basieren meist auf Content Filterung. Dies ist prinzipiell auch für Audioinhalte denkbar, wobei z.B. der Beginn einer Spit-Audiosequenz erkannt werden muss. Weitere mögliche Mechanismen, um sich vor SPIT zu schützen, sind [21]:

- **Filterung:** Klassifizieren von Anrufen anhand Ihrer Kennung. Filterung von SPIT-Anrufen anhand von Blacklists oder Beschränkung von eingehenden Anrufen auf in Whitelists vorgemerkte Kennungen.
- **Challenges:** Schutz vor automatischen Dialern durch Stellen einer zu lösenden Aufgabe am Telefon.
- **Authentizität:** Durch sichere Nummernzuordnung bzw. Verhindern von gefälschten Absenderdaten kann nur bekannten Teilnehmern das Absetzen von Anrufen erlaubt werden. Durch eine Umsetzung des Trapezoid Routing Konzepts [15] auf der Ebene der VoIP Anbieter können diese wiederum nur bekannten und vertrauenswürdigen Anbietern das Absetzen von Anrufen in das eigene Netz erlauben.
- **Kombinationen:** Sofern eine sichere Nummernzuordnung geschieht, könnte anhand von Blacklists und Whitelists bestimmt werden, welche Anrufe abgewiesen, welche direkt durchgestellt und welchen Anrufern eine Challenge gestellt werden soll.
- **Einverständnis:** Anrufe, deren Kennung weder zu Einträgen aus einer White- oder Blacklist zugeordnet werden können, durchlaufen eine zusätzliche Phase, in der der Angerufene den Anrufer zulassen oder abweisen kann – äquivalent zur Behandlung von unbekannten Gesprächspartnern bei Instant Messaging Systemen wie Skype.
- **Adressen sichern:** Ähnlich wie bei E-Mails sollten VoIP-Adressen nicht auf Internetseiten oder Diensten wie ENUM [9] direkt bzw. ungeschützt abfragbar sein, da dort so genannte Bots die Adressen automatisch erfassen und für SPIT verwenden können.
- **Rechtliche Grundlage:** Ohne expliziten Einsatz von Methoden zur Verschleierung ist es möglich, den Absender von SPIT zurück zu verfolgen. Mittels entsprechender Gesetze gegen SPIT (und internationaler Zusammenarbeit zu diesem Problembereich) liese sich eventuell das Versenden eingrenzen.

Mechanismus	**Vertraul.**	**Integrität**	**Authent.**	**Zugriffsk.**	**Verbindl.**	**Verfügb.**
Architektur						
L2/L1 Sicherheit	h	h		(h)		
DoS Protection						x
Stateful Firewall				x		
Intrusion Detection						x
Netzstruktur				x		x
Session Border C.			(x)	x		x
Protokolle						
IPsec / VPN	h	h	h	(h)		
TLS/SIPS	h,sig	h,sig	h,sig			
S/MIME	x,sdp	x,sig	x,sig		x,sig	
SRTP	x,media	x,media	x,media			
SCTP						x,sig
Authent./Digest		(x)	x	x	x	

Tab. 1: Mechanismen, überarbeitet von [26]
(h=nur Hop-by-Hop, sig= nur Signallisierung, sdp= nur SDP-Daten, media=nur Medienströme)

In der gezeigten Tabelle wurden die unterschiedlichen Mechanismen nochmals hinsichtlich ihrer Schutzwirkung und Anwendbarkeit klassifiziert.

3.6 VoIP-Sicherheitsanalyse Tools

Der Betreiber eines VoIP-Dienstes, der Administrator einer Firmenlösung, aber auch Heimnutzer benötigen Unterstützung bei der Absicherung ihrer Systeme. Ein dediziertes Werkzeug, das dies automatisiert vornimmt, existiert jedoch nicht. Durch eine Reihe von Analysewerkzeugen ist es jedoch möglich, ein eingerichtetes System auf Schwachstellen zu überprüfen. Wie in [4] und diesem Artikel gezeigt, sind eine Reihe der Angriffsmöglichkeiten nicht IP-Telefoniespezifisch – daher können hierfür auch generelle Netzwerkanalysewerkzeuge, wie SAINT [23], PROTOS [2] oder Nessus [1] verwendet werden (siehe auch [19]).

Neu hinzu kommen weitere Tools, welche VoIP spezifische Schwachstellen suchen. Der Voice over IP Security Scanner (SiVuS) ist einer der ersten erhältlichen Security-Scanner für VOIP Netzwerke basierend auf SIP. Das Programm wurde von vopsecurity.org entwickelt und steht auf www.vopsecurity.org zum freien Download bereit. SiVus ist dafür gedacht, Schwachstellen in einer Infrastruktur aufzudecken und zu bewerten, wie hoch das Sicherheitsrisiko ist. Dabei werden alle Bestandteile einer SIP-Infrastruktur auf Schwachstellen getestet, egal ob Soft-/Hardphones, Proxies, Registrars oder Redirect Server. Genutzt werden kann dieses Tool einerseits, um Sicherheitslücken zu erkennen und zu beseitigen, andererseits ist es gerade Angreifern durch Nutzung dieser Software möglich, diese Sicherheitslücken, sofern sie gefunden wurden, zu nutzen und darauf einen Angriff zu starten.

3.7 Security Pattern

Ein anderer sehr vielversprechender Ansatz ist die Verwendung von Security Pattern. Ein Pattern beschreibt dabei generisch eine in der Praxis etablierte Lösung für ein wiederkehrendes Problem. Security Pattern übertragen diesen Ansatz und stellen allgemeingültige Lösungsschemata für bestimmte Sicherheitsprobleme dar. Anhand der Beziehungen zwischen den Pattern können so Abhängigkeiten zwischen verschiedenen Teilproblemen erkannt werden. In [13] wird anhand einer Fallstudie die Anwendung von Security Pattern auf IP-Telefoniesysteme detailiert dargestellt.

3.8 Analyse

Im Zuge einer Umsetzung eines umfassenden Sicherheitskonzeptes gilt es darauf zu achten, dass sowohl Signalisierungs- als auch Mediendaten allen Sicherheitskriterien (Vertraulichkeit, Integrität, Authentifikation und Verbindlichkeit) unterliegen und dass bei den vermittelnden Systemelementen sowohl die Zugriffskontrolle als auch Verfügbarkeit gewährleistet werden kann. Manche Sicherheitsmechanismen lassen sich nur zur Hop-by-Hop Sicherung verwenden. Solche Mechanismen lassen sich nur dann sinnvoll einsetzen, wenn sichergestellt werden kann, dass alle durchlaufenen Entitäten im sicherheitsrelevanten Bereich vertrauenswürdig sind.

Unter den direkt vom SIP-Standard unterstützten Sicherheitsverfahren ist S/MIME das technisch fortschrittlichste. Durch die Verschlüsselung von Nachrichten-Rümpfen wird es Angreifern erschwert, die darin enthaltenen SDP-Information, wie die SIP URIs, IP- und Port Adressen beider Parteien, die Standorte der Parteien und die Tatsache, dass die Parteien miteinander

telefonieren mitzulesen. Durch den Einsatz digitaler Signaturen wird auch die Ende-zu-Ende Integrität der Nachrichten erreicht.

Diese technischen Vorteile scheitern aber leider zum Teil auch an organisatorischen Problemen. Es gibt auf Grund des komplexen Verfahrens und der geringen Anwendung derzeit wenige Implementierungen der genannten Sicherheitsmechanismen für Soft- und Hardphones.

Ein weiteres Problem ist, dass das asymmetrische Verschlüsseln von Nachrichten die vorherige Kenntnis des öffentlichen Schlüssels des Angerufenen voraussetzt. Dieser Schlüssel, der z.B. in einem X.509 Zertifikat enthalten sein kann, muss von dem Angerufenen vorher durch spezielle SIP-Anfragen beschafft oder bei einem öffentlichen Verzeichnis (Public-Key-Infrastructure – PKI) angefragt werden. Ein Problem aber stellt die umfassende Umsetzung einer PKI dar. Sie benötigt sog. Trusted Third Parties, also vertrauenswürdige Zertifizierungsstellen, um Zertifikate auszustellen, zu prüfen und zurückzuziehen. Zum einen gibt es bisher keine globale Zertifizierungsstelle, die diese Aufgaben wahrnimmt, sondern mehrere lokale und zum anderen ist der Erwerb eines X.509 Zertifikates von einer großen Zertifizierungsstelle eine relativ schwierige und vor allem kostspielige Angelegenheit, so dass derzeit wenige Nutzer ein individuelles Zertifikat besitzen.

4 Zusammenfassung und Vorgehensempfehlung

Der Aufbau eines sicheren VoIP Systems ist nicht trivial. Durch eine unbedachte Integration eines VoIP Systems in ein bestehendes, sicheres Netzwerk können neuartige und zusätzliche Sicherheitslücken in ein Netzwerk eingeführt werden. Noch gibt es keine allgemeingültige Lösung für alle Schwachstellen eines VoIP Systems. Im Vorfeld sollte klar sein, welche Randbedingungen und Anforderungen an das System bestehen, welche Sicherheitsziele erfüllt sein müssen und welcher Aufwand dafür betrieben werden kann. Dafür sollten diese Probleme geklärt, analysiert und entsprechende Mechanismen ausgewählt werden, bevor ein System aufgebaut werden kann, welches die Sicherheitsansprüche erfüllt.

Literatur

[1] NESSUS. http://www.nessus.org.

[2] PROTOS - Security Testing of Protocol Implementation. http://www.ee.oulu.fi/research/ouspg/protos/index.html.

[3] ITU H.232 Standard, 2005. http://www.packetizer.com/voip/h323/standards.html.

[4] Ralf Ackermann, Markus Schumacher, Utz Roedig, and Ralf Steinmetz. Vulnerabilities and Security Limitations of current IP Telephony Systems. In *Proceedings of the Conference on Communications and Multimedia Security (CMS 2001), Darmstadt*, pages 53–66, May 2001.

[5] Salman A. Baset and Henning Schulzrinne. An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol, September 2004. http://arxiv.org/ftp/cs/papers/0412/0412017.pdf.

[6] Baugher, McGrew, Carrara, Naslund, and Norrman. The Secure Real-time Transport Protocol. Internet Draft draft-ietf-avt-srtp-09, Internet Engineering Task Force, July 2003. Work in progress.

[7] M. Baugher. The Secure Real-time Transport Protocol (SRTP). Request for Comments 3711, Network Working Group, 2004.

[8] T. Dieks and C. Allen. The TLS Protocol – Version 1.0. Request for Comments 2246, Internet Engineering Task Force, 1999.

[9] P. Faltstrom. The E.164 to Uniform Resource Identifiers / Application (ENUM). Request for Comments 3761, Internet Engineering Task Force, April 2004.

[10] J. Franks. Request for Comments: 2617 HTTP Authentication: Basic and Digest Access Authentication. Request for Comments 2617, Internet Engineering Task Force, 1999.

[11] Bundesministerium für Sicherheit in der Informationstechnik. VoIP. http://www.bsi-fuer-buerger.de/intern_telefon/voice_over.htm.

[12] Deloitte & Touche GmbH. Am Start. Auswirkungen von Voice over IP auf den deutschen Telekommunikationsmarkt.

[13] Manuel Görtz. *Security Patterns – Integrating Security and Systems Engineering*, chapter Case Study: IP Telephony. Wiley & Sons, 2005. to appear.

[14] IDC. Worldwide VoIP Management 2005-2009 Forecast Update. http://www.idc.com/getdoc.jsp?containerId=34198.

[15] Jan Janak. SIP Introduction, 2003. http://www.iptel.org/ser/doc/sip_intro/sip_introduction.html.

[16] C. Jennings. Example call flows using sip security mechanisms. Internet draft, Network Working Group, October 2003.

[17] S. Kent and R. Atkinson. Security Architecture for the Internet Protocol. Request for Comments 2401, Internet Engineering Task Force, November 1998.

[18] Klaus Lenssen. Sichere IP-Telefonie durch verteilte Maßnahmen, January 2005. http://www.voipmagazin.de/magazin/ artikel_613_sicherheit_voip_ip_telefonie_massnahmen.html.

[19] Jürgen Plate and Jörg Holzmann. Sicherheit in Netzen, Tools und Quellen. http://www.netzmafia.de/skripten/sicherheit/sicher8.html.

[20] B. Ramsdell. S/MIME Version 3 Message Specification. Request for Comments 2633, Internet Engineering Task Force, June 1999.

[21] J. Rosenberg and C. Jennings. The Session Initiation Protocol (SIP) and Spam. Internet Draft, July 2005.

[22] Jonathan Rosenberg, Henning Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler. SIP: Session Initiation Protocol. Request for Comments 3261, Internet Engineering Task Force, June 2002.

[23] Saint Corp. Security Administrators Integrated Network Tool. http://www.saintcorporation.com/products/saint_engine.html.

[24] Henning Schulzrinne, S. Casner, R. Frederick, and V. Jacobson. RTP: A Transport Protocol for Real-Time Applications. Request for Comments 1889,3550, Internet Engineering Task Force, January 1996.

[25] R. Stewart, Q. Xie, K. Morneault, C. Sharp, H. Schwarzbauer, T. Taylor, I. Rytina, M. Kalla, L. Zhang, and V. Paxson. Stream Control Transmission Protocol. Request for Comments 2960, Internet Engineering Task Force, October 2000.

[26] U. Trick and F. Weber. SIP, TCP/IP und Telekommunikationsnetze, 2005.

[27] VOIPSA. VoIP Security Alliance, 2005. http://www.voipsa.org.